Commentary—authoritarianism special issue

Dialogues on Digital Society
1–5

DOI: 10.1177/29768640251382644
journals.sagepub.com/home/dds
Sage

Smart infrastructure, techno-authoritarianism, and the threat to democracy in Brazil

Jess Reia
School of Data Science, University of Virginia

Abstract

This commentary examines how Brazil's smart city agenda enables techno-authoritarianism, drawing on eight years of fieldwork and policy and legal analysis. It focuses on the use of surveillance technologies and the influence of foreign and local tech companies in shaping urban governance through opaque, corporate-led policymaking. It discusses how smart infrastructures are deployed under the guise of innovation, often bypassing democratic processes and civic participation. These developments reflect a broader global trend of "technosolutionist urbanism," where digital infrastructure is used to monitor, control, and commodify residents. The Brazilian case underscores the urgent need for a justice-based, transparent, and participatory framework for smart infrastructure governance, centering human rights and democratic accountability in the face of rising techno-authoritarianism.

Keywords

Techno-authoritarianism, smart city, democracy, Brazil, surveillance, lobbying

Introduction

In June 2025, the Brazilian Supreme Federal Court released a report prepared by the federal police detailing the findings of an investigation into the clandestine intelligence operations undertaken during Jair Bolsonaro's presidency. Leading an authoritarian, far-right government that overlooked and weakened democratic institutions, Bolsonaro created a vast surveillance network targeting scholars, activists, journalists, and opposing politicians. His administration used the Brazilian Intelligence Agency (ABIN) to monitor people illegally, relying on the FirstMile software developed by Israeli company Cognyte (Domenici, 2025). FirstMile can detect an individual based on the location of devices by using mobile networks, and it was used to monitor around 10,000 people over 12 months (EFF, 2023). Public outcry followed the court report, shedding light on other ongoing surveillance projects and questioning the role of foreign tech companies in the undermining of Brazilian democracy.

This case is an example of how the global trend toward techno-authoritarianism (LaFrance, 2024; Lamensch, 2022) manifests in Brazil (Pinheiro-Machado and Vargas-Maia, 2023) and how it is rooted in the influence of corporate power on governmental technology acquisition. The deployment

Corresponding author:
Jess Reia, School of Data Science, UVA, 1919 Ivy Road, Charlottesville, VA, USA.
Email: reia@virginia.edu

of so-called smart solutions is part of a broader, transnational smart city technopolitical agenda (Kurban et al., 2017) that has been in place for over a decade and vastly studied from a critical perspective (Antenucci, 2021; Datta, 2018; Morozov and Bria, 2018). Smart city infrastructures can threaten local and regional democracy by allowing corporate interests and storytelling (Sadowski and Bendor, 2019; Söderström et al., 2014) to prevail in law and policymaking while providing powerful monitoring tools to authoritarian governments.

Drawing from eight years of fieldwork in Brazilian smart cities and expos, as well as legal and policy tracking, this commentary presents a few examples of how the smart infrastructure technopolitical agenda can undermine democracy. It focuses on two concerning trends that have become a political party platform during elections: consultancy firms and companies drafting municipal laws disguised as "master plans for smart cities and innovation" (Juazeiro do Norte, 2018) that disregarded data protection (Reia and Cruz, 2025); and, simultaneously, the rise of facial recognition technologies (FRT) and other surveillance tools as alleged solutions to violence.

The corporate-led smart city agenda in Brazil

The corporate-led policy and lawmaking taking place at the city level in Brazil is shaped when consultancy firms draft municipal laws under a "smart city masterplan" disguise that often treats data as a commodity to be exploited for private interests while increasing surveillance. Attention is rightfully directed at big tech companies (such as IBM, Cisco, Huawei, Amazon, and Microsoft). Indeed, Brazil is pursuing the development of smart infrastructure through controversial policies to attract data centers, which will be operated by foreign companies, with a promise to create jobs and promote innovation, and a dismissive approach to the impact they have on ecosystems, communities, and resources (IP.Rec, 2025). However, the Brazilian case also shows us that local companies and consultancy firms are quietly facilitating the privatization of cities. Consultancy firms such as SPin signed multi-million Brazilian Real contracts to draft master plans for smart cities that end up enshrined as municipal law in Juazeiro do Norte (2018), Vitória (2020), and Salvador (2022). These laws are not going through the regular democratic processes that involve elective officials and legislative chambers, benefiting from loopholes, the lack of lobbying regulation in the country, and the promotion of public–private partnerships as governmental efficiency. They also do not involve residents in the process, with flawed or nonexistent civic engagement opportunities.

As various cities face the increasing impact of climate change and the outcomes of historical inequalities, the promises of foreign investment and data-centered solutions are alluring. Local governments' adoption of smart technologies is not new, but it is a practice accelerated by the recent popularity of artificial intelligence (AI) models (Yigitcanlar et al., 2024), especially predictive AI tools and FRT. In Brazil, the establishment of expos and rankings pushed the smart city technopolitical agenda beyond large metropolitan areas, feeding the growing market of smartness. Surveillance systems such as FRT are driving this agenda, sold as a tool to tackle crime but being challenged by human rights organizations for privacy issues and their abuse by authoritarian governments (Nunes et al., 2025).

Surveillance systems and smart city authoritarianism

For prioritizing technology as an end in itself to solve urban problems, we can call the corporate smart cities agenda "technosolutionist urbanism" (Reia and Cruz, 2025). The technosolutionist urbanism approach often uses foreign software and hardware from countries such as Russia, China, Israel, and the United States (Access Now, 2021), which not only fails to incentivize local innovation, but also poses cybersecurity (Hurel, 2023) and digital sovereignty (Santaniello, 2025) threats. Opaque relationships between authoritarian governments and the private sector allow for the development

of control over residents without transparency or accountability mechanisms, and grant companies power over infrastructure and citizen data.

Despite having a robust regulatory framework for data protection (LGPD) inspired by the European General Data Protection Regulation and built on years of multistakeholder deliberation, the disregard for transparency in Bolsonaro's mandate took many forms. It was reflected in the denial of Freedom of Information Act-equivalent requests (Tecnoblog, 2022) and imposition of a 100-year secrecy on public data (BBC News Brasil, 2022) —actions that were copied at the state and municipal levels. Beyond regulation, Brazil is home to vibrant civil society organizations focusing on digital rights. However, instead of proposing a positive agenda, as was the case with the Civil Rights Framework for the Internet and the LGPD, public interest advocacy had to deal with the backslide of the democratic process, highlighting that authoritarian practices can flourish despite strong civil society work and collectively built regulatory frameworks. To tackle techno-authoritarianism, other laws need to be revised or created, from lobbying regulation to procurement policies.

Intertwined in the first trend, FRT comes to mind as a relevant second example of how smart infrastructure can serve authoritarianism. In Brazil, one of the most notable cases is the Smart Sampa program in the city of São Paulo.[1] When the public tender was made available in 2022, the main goal of Smart Sampa was to install and integrate over 20,000 surveillance cameras by 2024, to make the city "smarter" by improving predictive public security. The document also mentioned monitoring the social media of residents. The process was questioned by a coalition of over 50 civil society organizations due to the threats to human rights and democracy that such a massive surveillance system would cause (Martins, 2022). The public tender was suspended, revised, and faced scrutiny from advocates, scholars, and journalists. In 2023, when the company to be hired was announced, it was one involved in many corruption cases in the country (Rebello, 2023).

The development of vast networks for monitoring, surveilling, and controlling residents opens the door to potential misuse, abuse, and corruption. As the ABIN case mentioned in the beginning, alternative or parallel illegal operations targeting dissidence happen within existing infrastructures and organizations. Smart Sampa is one of many projects focused on acquiring and deploying FRT systems in cities of all sizes that sometimes do not have basic infrastructure, such as sewage treatment (Rebello, 2023a). Yet, as the country failed to regulate AI and establish safeguards for human rights in the aftermath of an authoritarian government, it is key to reflect on the role of digital technologies in facilitating authoritarian rule. For example, in June 2025, Meta and Google offered workshops on how to leverage AI for election campaigns for Bolsonaro's far-right party ("Partido Liberal") (De Sousa, 2025) by facilitating its use in political communication.

Overall, smart cities can be a threat to democracy because they "employ a host of technologies that can be used inappropriately, jeopardizing basic civil liberties and political rights" (Da Vinha, 2023: 2). With upcoming elections in which the far-right has a strong presence, Brazil must consider tackling techno-authoritarianism to secure its democratic institutions and processes. To do so, it is important to address the "lack of political situatedness" (Akbari, 2022: 444) of smart tech, situating smart infrastructure within political regimes.

Conclusion

The conclusions we might draw here are twofold. First, corporate-led law and policymaking, as well as unregulated lobbying, are creating more opportunities for the acquisition and deployment of deeply problematic, surveillance-centered smart infrastructure. With little to no social participation and accountability, these projects do not (and cannot) serve the public interest. Second, the increasing closeness of big tech companies to authoritarian leaders and parties needs special attention, as platforms can be made available to law enforcement to monitor citizens and non-citizens. Brazil has a strong civil society that could help develop a human rights, justice-based framework for smart infrastructure governance and reassess what kind of smart infrastructure cities, states, and

the federal government need—or if they are needed at all. Critically assessing what we consider smartness to be, dissecting the role of AI and predictive tools, and working collectively in multistakeholder approaches are more important for democracy than ever.

Acknowledgments

Thank you to Luã Cruz for the long-term collaboration that resulted in some ideas presented here and to Pedro A. P. Francisco and Ana Brandusescu for the comments provided to the first draft.

Declaration of conflicting interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Ethical approval and informed consent statements

There are no human participants in this commentary, and informed consent is not required.

Funding

The author disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was partially funded by the Open Society Foundations and the UVA School of Data Science.

ORCID iD

Jess Reia https://orcid.org/0000-0002-6023-4584

Note

1. See: https://smartsampa.prefeitura.sp.gov.br/. Residents can integrate their residential or commercial cameras into the system.

References

Access Now. (2021) Surveillance tech in Latin America: made abroad, deployed at home. Report, Access Now, August.

Akbari A (2022) Authoritarian smart city: a research agenda. *Surveillance & Society* 20(4): 441–449.

Antenucci I (2021) Infrastructures of extraction in the smart city: zones, finance, and platforms in New Town Kolkata. *International Journal of Communication* 15: 2652–2668.

BBC News Brasil. (2022) O que é sigilo de cem anos imposto por Bolsonaro e atacado por Lula. BBC News Brasil, 31 August. Available at: https://www.bbc.com/portuguese/brasil-62722610

Datta A (2018) The digital turn in postcolonial urbanism: smart citizenship in the making of India's 100 smart cities. *Transactions of the Institute of British Geographers* 43(3): 405–419.

da Vinha L (2023) Smart cities: the prospects of digital authoritarianism. JBC Policy Perspectives #4, Flinders University, September.

de Sousa S (2025) Treinamento de guerra. *The Intercept Brasil*, 4 Jun. Available at: https://www.intercept.com.br/2025/06/04/oficinas-google-meta-partido-bolsonaro/.

Domenici T (2025) Abin Paralela, como tudo se conecta: espionagem, FirstMile, Bolsonaros e Ramagem. Pública, 17 June. Available at: https://apublica.org/2025/06/abin-paralela-como-tudo-se-conecta-espionagem-firstmile-bolsonaros-e-ramagem/

EFF. (2023) Recent surveillance revelations, enduring Latin American issues. Electronic Frontier Foundation, 25 December. Available at: https://www.eff.org/deeplinks/2023/12/recent-surveillance-revelations-enduring-latin-american-issues-2023-year-review

Hurel LM (2023) Mapping cyber policy in Latin America: the Brazilian case. Report, Centro LATAM Digital, April.

IP.Rec. (2025) *IA, data centers e os impactos ambientais*. Policy brief, IP.Rec., Recife, Brazil.

Juazeiro do Norte. (2018) Lei Complementar N° 117, de 11 de junho de 2018. Diário Oficial do Município. Juazeiro do Norte, CE, Caderno I do dia 14 de junho de 2018, ano XX, n° 4762:2.

Kurban C, Peña-López I and Haberer M (2017) What is technopolitics? A conceptual scheme for understanding politics in the digital age. IDP. *Revista de Internet, Derecho y Ciencia Política* 24: 3–20.

LaFrance A (2024) The rise of techno-authoritarianism. The Atlantic, 30 January. Available at: https://www.theatlantic.com/magazine/archive/2024/03/facebook-meta-silicon-valley-politics/677168/

Lamensch M (2022) In Brazil, "Techno-Authoritarianism" rears its head. Centre for International Governance Innovation, 19 September. Available at: https://www.

cigionline.org/articles/in-brazil-techno-authoritarianism-rears-its-head/

Martins L (2022) Idec e mais de 50 organizações acionam MP contra edital da Prefeitura de SP que quer contratar sistema de monitoramento facial. G1, 30 November. Available at: https://g1.globo.com/sp/sao-paulo/noticia/2022/11/30/idec-e-mais-de-50-organizacoes-acionam-mp-contra-edital-da-prefeitura-de-sp-que-quer-contratar-sistema-de-monitoramento-facial.ghtml

Morozov E and Bria F (2018) *Rethink the smart city: Democratizing urban technology*. Berlin, Germany: Rosa Luxemburg Stiftung.

Nunes P, Travassos do Carmo GS, Lima T, et al. (2025) *Mapeando a vigilância biométrica: levantamento nacional sobre o uso do reconhecimento facial na segurança pública*. Rio de Janeiro: CESeC.

Pinheiro-Machado R and Vargas-Maia T (2023) *The Rise of the Radical Right in the Global South*. London, UK and New York, NY: Routledge.

Rebello A (2023) Crise de imagem. *Intercept Brasil*, 16 Ago. Available at: https://www.intercept.com.br/2023/08/14/smart-sampa-denunciada-por-corrupcao-capturar-seu-rosto-em-sp/

Rebello A (2023a) O mecenas. Intercept Brasil, 5 April. Available at: https://www.intercept.com.br/2023/04/05/delegado-waldir-torrou-r-30-milhoes-em-reconhecimento-facial-para-cidades-que-sequer-tem-saneamento-em-goias/

Reia J and Cruz L (2025) Smart-Washing the city: a study on the privatization of urban digital infrastructures in the global south. *International Journal of Communication* 19(23): 930–952.

Sadowski J and Bendor R (2019) Selling smartness: corporate narratives and the smart city as a sociotechnical imaginary. *Science, Technology, & Human Values* 44(3): 540–563.

Salvador (2022) *Plano diretor de tecnologias da cidade inteligente*. Salvador, Brazil: Prefeitura de Salvador.

Santaniello M (2025) Attributes of digital sovereignty: a conceptual framework. *Geopolitics*: 1–22.

Söderström O, Paasche T and Klauser F (2014) Smart cities as corporate storytelling. *City* 18(3): 307–320.

Tecnoblog. (2022) Governo Bolsonaro está usando LGPD como pretexto para esconder dados. *IG*, 5 April. Available at: https://tecnologia.ig.com.br/colunas/tecnoblog/2022-04-05/governo-bolsonaro-usa-lgpd-ocultar-informacoes.html

Vitória (2020) *Plano Diretor de Tecnologia para Cidades Inteligentes de Vitória—PDTCI*. Vitória, Brazil: Prefeitura de Vitória.

Yigitcanlar T, Senadheera S, Marasinghe R, et al. (2024) Artificial intelligence and the local government: a five-decade scientometric analysis on the evolution, state-of-the-art, and emerging trends. *Cities* 152: 105151.